



E-COMMERCE PROTECTION – A LIFE SUCCESSION ADVANCE

Dr Kinjalkumar Narendrabhai Mistri

I/C Principal, Shri Mansukhbhai J Medani B.b.a College, Kalol, Guajart University, Ahmadabad

ABSTRACT

- The rapid evolution of computing and communication technologies and their standardizations have made the boom in e-commerce possible. Lowering of the cost of operation, increase in the speed of transactions, and easy global reach to customers and vendors have been the reasons for the overwhelming popularity of this new way of commerce. This article examines the issues related to the security of the assets and transactions in the e-commerce components and activities. Since large public money is involved in the transactions, the role of information security and privacy is not exaggerated in this kind of business.
- After examining the technologies used in e-commerce, the article goes on to identify the security requirement of ecommerce systems from perceived threats and vulnerabilities. Then e-commerce security is viewed as an engineering management problem and a life cycle approach is put forward. How the e-commerce systems can be made secure using the life cycle approach is outlined. The relevant standards and laws are also discussed in the perspective of e-commerce. The article closes with some future research directions and conclusions.

KEYWORDS: E-Commerce Security; Threats and Vulnerabilities; Security Engineering Life Cycle; Security Standards; IT Act.

INTRODUCTION TO E-COMMERCE

- To many people, the term electronic commerce (sometimes shortened to e-commerce) (Kalakota & Whinston 1999) means shopping in the part of the internet called the World Wide Web. However, e-commerce has a much broader scope and encompasses many more business activities other than just web shopping. Some people and businesses use the term electronic business (or e-business) when they are talking about e-commerce in this broader sense. In this paper, we will use the term e-commerce in its broadest definition. Although the web has made online shopping possible for many businesses and individuals, in a broader sense, e-commerce has existed for many years. For decades, banks have been
- using electronic funds transfers (EFTs) (Schneider & Perry 2001), which are electronic transmissions of account exchange information over private communications networks. Businesses also have been engaging in a form of e-commerce, known as electronic data interchange (EDI), for many years. EDI occurs when one business transmits computer readable data in standard format to another business. In the 1960s, businesses realized that many of the documents they exchanged related to the shipping of goods – such as invoices, purchase orders, and bills of lading – and included the same set of information for almost every transaction. They also realized that they were spending a good deal of time and money entering these data into their computers, printing paper forms, and then re-entering the data on the other side of the transaction. Although the purchase order, invoice, and bill of lading for each transaction contained much of the same information, each paper form had its own unique format for presenting that information. By creating a set of standard formats for transmitting that information electronically, businesses were able to reduce errors, avoid printing and mailing costs, and eliminate the need to re-enter data. Businesses that engage in EDI with each other are called trading partners.
- The standard formats used in EDI contain the same information that businesses have always included in their standard paper invoices, purchase orders, and shipping documents. A good definition of e-commerce would mention the use of electronic data transmission to implement or enhance any business process. Some people use the term “internet commerce” to mean e-commerce that specifically uses the internet or the web as its data transmission medium. IBM has defined electronic business to be “the transformation of key business processes through the use of Internet technologies”.

Advantages of E-Commerce

- The advantages of e-commerce for business entities can be summarized thus: e-commerce can increase sales and decrease costs. A firm can use e-commerce to reach narrow market segments that are widely scattered geographically. The internet and the web are particularly useful in creating virtual communities that become ideal target markets. A virtual community is a gathering of people who share a common interest, but, instead of this gathering occurring in the physical world, it takes place on the internet. Just as e-commerce

increases sales opportunities for the seller, it increases purchasing opportunities for the buyer. Businesses can use e-commerce in their purchasing processes to identify new suppliers and business partners. Negotiating price and delivery terms is easier in e-commerce, because the web can provide competitive bid information very efficiently. e-Commerce increases the speed and accuracy with which businesses can exchange information, which reduces costs on both sides of transactions.

E-Commerce provides buyers with a wider range of choices than traditional commerce, because they can consider many different products and services from a wider variety of sellers. The benefits of e-commerce also extend to the general welfare of society. Electronic payments of tax refunds, public retirement, and welfare support cost less to issue and arrive securely and quickly when transmitted via the Internet. Furthermore, electronic payments can be easier to audit and monitor than payments made by check, which can help protect against fraud and theft losses. e-Commerce can make products and services available in remote areas. For example, distance education is making it possible for people to learn skills and earn degrees no matter where they live or what hours of the day they have available for study.

Disadvantages of E-Commerce

- E-Commerce also has its disadvantages. It is difficult to conduct a few businesses electronically. For example, perishable foods and high-cost items such as jewellery or antiques may be impossible to adequately inspect from a remote location, regardless of the technologies that are devised in the future. However, most of the disadvantages of e-commerce today are due to the newness and rapidly developing pace of the underlying technologies. Return on investment numbers is difficult to compute for investments in e-commerce, because the costs and benefits are hard to quantify. Costs, which are a function of technology, can change dramatically during even short-lived e-commerce implementation projects, because the underlying technologies change rapidly. In addition to technology issues, many businesses face cultural and legal impediments to e-commerce. Some consumers are still somewhat fearful of sending their credit card numbers over the Internet.
- The legal environment in which e-commerce is conducted is full of unclear and conflicting laws. In many cases, government regulators have not kept up with technologies. As more businesses and individuals find the benefits of e-commerce compelling, many of these technology- and culture-related disadvantages will disappear. Another important issue is security. Transactions between buyers and sellers in e-commerce include requests for information, quotation of prices, placement of orders and payment, and sales services. The high degree of confidence needed in the authenticity, confidentiality, and timely delivery of such transactions can be difficult to maintain where they are exchanged over the Internet. The interception of transactions, and in particular credit card details, during transmission over the Internet is often a major obstacle to public confidence in e-

commerce.

E-Commerce Technologies

- Several technologies are needed for e-commerce to exist. The most obvious one is the internet. Beyond that system of interconnected networks, many other sophisticated software and hardware components are needed to provide the required support structure: database software, network switches and hubs, encryption hardware and software, multimedia support, and the world wide web. Methods of connecting all the software and hardware elements in just the right way to support electronic commerce are changing and evolving everyday. The rate of change is rapid for all elements that support electronic commerce.

Characteristics of E-Commerce Technologies

The following are the characteristics of e-commerce technologies (Burns 2002):

- Ease of automated processing:** A payer can now easily automate the generation and processing of multiple payments with minimal effort and cost. Previously, the dependency upon banks to handle most payments and the lack of a cheap, ubiquitous communications technology made automation of payment processes expensive and difficult to establish.
- Immediacy of result:** Payment immediacy occurs because of automation and the ability of the intermediate systems and providers to process payments in real-time. In manual, paper based systems there exists a time delay due to the requirement of human intervention in the process.
- Openness and accessibility:** The availability of cheap computing and communications technology, and appropriate software enables small enterprises and individuals to access or provide a range of payment services that were previously only available to large organizations via dedicated networks or the transactional processing units of banks.
- Loss of collateral information:** The new technology dispenses with, or alters, collateral information accompanying transactions. This information has traditionally been part of the transaction, and has been relied upon by the transacting parties to validate individual payments.
- Globalization:** Globalization, or the minimization of geographical factors in making payments, is an obvious aspect of the new payments systems. Its effect is upon areas such as size of the payments marketplace, uncertainty as to legal jurisdiction in the event of disputes, location and availability of transaction trails, and the ability of a payment scheme to rapidly adapt to regulatory regimes imposed by one country by moving to another.
- New business models:** New business models are being developed to exploit the new payment technologies, in particular to address or take advantage of the disintermediation of customers from traditional payment providers such as banks. Disintermediation is where the technology enables a third party to intervene between the customer and the banking system, effectively transferring the customer's trusted relationship with the bank to the new party.

Security Threats to E-Commerce – Requirements Definition

- E-Commerce security requirements can be studied by examining the overall process, beginning with the consumer and ending with the commerce server. Considering each logical link in the "commerce chain", the assets that must be protected to ensure secure e-commerce include client computers, the messages travelling on the communication channel, and the web and commerce servers – including any hardware attached to the servers. While telecommunications are certainly one of the major assets to be protected, the telecommunications links are not the only concern in computer and e-commerce security.
- Client threats:** Until the introduction of executable web content, Web pages were mainly static. Coded in HTML, static pages could do little more than display content and provide links to related pages with additional information. However, the widespread use of active content has changed this perception.
- Active content:** Active content refers to programs that are embedded transparently in web pages and that cause action to occur. Active content can display moving graphics, download and play audio, or implement web-based spreadsheet programs. Active content is used in e-commerce to place items one wishes to purchase into a shopping cart and to compute the total invoice amount, including sales tax, handling, and shipping costs. The best known active content forms are Java applets, ActiveX controls, JavaScript, and VB Script. Since active content modules are embedded in web pages, they can be completely transparent to anyone browsing a page containing them. Anyone can embed malicious active content in web pages. This delivery technique, called a trojan horse, immediately begins executing and taking actions that cause harm. Embedding active content to web pages involved in e-commerce introduces

several security risks.

- Malicious codes:** Computer viruses, worms and trojan horses are examples of malicious code. A trojan horse is a program which performs a useful function, but performs an unexpected action as well. Virus is a code segment which replicates by attaching copies to existing executables. A worm is a program which replicates itself and causes execution of the new copy. These can create havoc on the client side.
- Server-side masquerading:** Masquerading lures a victim into believing that the entity with which it is communicating is a different entity. For example, if a user tries to log into a computer across the internet but instead reaches another computer that claims to be the desired one, the user has been spoofed. This may be a passive attack (in which the user does not attempt to authenticate the recipient, but merely accesses it), but it is usually an active attack (in which the masquerader issues responses to mislead the user about its identity).
- Confidentiality threats:** Confidentiality is the prevention of unauthorized information disclosure. Breaching confidentiality on the internet is not difficult. Suppose one logs onto a website – say www.anybiz.com – that contains a form with text boxes for name, address, and e-mail address. When one fills out those text boxes and clicks the submit button, the information is sent to the web-server for processing. One popular method of transmitting data to a web-server is to collect the text box responses and place them at the end of the target server's URL. The captured data and the HTTP request to send the data to the server is then sent. Now, suppose the user changes his mind, decides not to wait for a response from the anybiz.com server, and jumps to another website instead – say www.somecompany.com. The server somecompany.com may choose to collect web demographics and log the URL from which the user just came. By doing this, somecompany.com has breached confidentiality by recording the secret information the user has just entered.
- Integrity threats:** An integrity threat exists when an unauthorized party can alter a message stream of information. Unprotected banking transactions are subject to integrity violations. Cyber vandalism is an example of an integrity violation. Cyber vandalism is the electronic defacing of an existing website page. Masquerading or spoofing – pretending to be someone you are not or representing a website as an original when it really is a fake – is one means of creating havoc on websites. Using a security hole in a domain name server (DNS), perpetrators can substitute the address of their website in place of the real one to spoof website visitors. Integrity threats can alter vital financial, medical, or military information. It can have very serious consequences for businesses and people.
- Availability threats:** The purpose of availability threats, also known as delay or denial threats, is to disrupt normal computer processing or to deny processing entirely. For example, if the processing speed of a single ATM machine transaction slows from one or two seconds to 30 seconds, users will abandon ATM machines entirely. Similarly, slowing any internet service will drive customers to competitors' web or commerce sites.
- Server threats:** The server is the third link in the client-internet-server trio embodying the e-commerce path between the user and a commerce server. Servers have vulnerabilities that can be exploited by anyone determined to cause destruction or to illegally acquire information.
- Web-server threats:** Web-server software is designed to deliver web pages by responding to HTTP requests. While web-server software is not inherently high-risk, it has been designed with web service and convenience as the main design goal. The more complex the software is, the higher the probability that it contains coding errors (bugs) and security holes – security weaknesses that provide openings through which vildowers can enter.
- Commerce server threats:** The commerce server, along with the web-server, responds to requests from web browsers through the HTTP protocol and CGI scripts. Several pieces of software comprise the commerce server software suite, including an FTP server, a mail server, a remote login server, and operating systems on host machines. Each of this software can have security holes and bugs.
- Database threats:** E-commerce systems store user data and retrieve product information from databases connected to the web-server. Besides product information, databases connected to the web contain valuable and private information that could irreparably damage a company if it were disclosed or altered. Some databases store username/password pairs in a non-secure way. If someone obtains user authentication information, then he or she can masquerade as a legitimate database user and reveal private and costly information.
- Common gateway interface threats:** A common gateway interface (CGI) implements the transfer of information from a web-server to another program, such as a database program. CGI and the programs to which they transfer data provide active content to web pages. Because CGIs are programs, they present a security threat if

misused. Just like web-servers, CGI scripts can be set up to run with their privileges set to high – unconstrained. Defective or malicious CGIs with free access to system resources are capable of disabling the system, calling privileged (and dangerous) base system programs that delete files, or viewing confidential customer information, including usernames and passwords.

13. **Password hacking:** The simplest attack against a password-based system is to guess passwords. Guessing of passwords requires that access to the complement, the complementation functions, and the authentication functions be obtained. If none of these have changed by the time the password is guessed, then the attacker can use the password to access the system.

Security engineering life cycle

- It is important to note that the e-commerce security need of an enterprise is dynamic rather than static and depends on the operational dynamics, shift or addition to business goals, technological advancement etc. Thereby, the process of designing and deploying an information security infrastructure is a continuous process of analysis, design, monitoring, and adaptation to changing needs. Often, the change in needs is frequent in the organizations. In order to figure 1. Security engineering life cycle. Be survivable under such frequent changes, the process has to be developed from a life-cycle approach. This observation leads to the concept of “security engineering life-cycle” (mazumdar et al 2003). The security engineering life cycle consists of the following phases (figure 1):

Security requirement specification and risk analysis: This is the first phase in the security engineering life cycle. It collects information regarding assets of the organization that need to be protected, threat perception on those assets, associated access control policies, existing operational infrastructure, connectivity aspects, services required to access the asset and the access control mechanism for the services.

1. **Security policy specification:** This phase uses “security requirement specification” and “risk analysis report” as input and generates a set of e-commerce security policies. The policy statements are high-level rule-based and generic in nature, and, thereby, does not provide any insight to system implementation or equipment configuration.
2. **Security infrastructure specification:** This phase analyses the “security requirement specification” and the “security policy specification” to generate a list of security tools that are needed to protect the assets. It also provides views on the location and purpose of the security tools.
3. **Security infrastructure implementation:** The organization, in this phase, procures, deploys, and configures the selected security infrastructure at the system level.
4. **Security testing:** In this phase, several tests are carried out to test the effectiveness of the security infrastructure, functionality of the access control mechanism, specified operational context, existence of known vulnerabilities in the infrastructure etc.
5. **Requirement validation:** This phase analyses the extent of fulfillment of the security requirements of the e-commerce organization by the corresponding security policy and the implemented security infrastructure. Change in the business goal, operational environment, and technological advancement may lead to a fresh set of security requirements and thereby, triggering a new cycle of the “security engineering life cycle”. Now, let us see the Security Requirements, Security Policy, Security Infrastructure, and Security Testing phases in greater detail.

Security requirements

During this phase, the security needs of an enterprise are identified. These needs are governed by the necessity to protect the following security attributes:

1. **Authentication:** This is the ability to say that an electronic communication (whether via email or web) does genuinely come from who it purports to. Without face-to-face contact, passing oneself off as someone else is not difficult on the internet. Forging the “From:” field in an email header is a trivial matter, and far more sophisticated attacks are standard fare for hackers. In online commerce the best defence against being misled by an imposter is provided by unforgeable digital certificates from a trusted authority (such as VeriSign). Although anyone can generate digital certificates for themselves, a trusted authority demands real-world proof of identity and checks its validity before issuing a digital certificate. Only certificates from trusted authorities will be automatically recognized and trusted by the major web browser and email client software. Authentication can be provided in some situations by physical tokens (such as a driver's license), by a piece of information known only to the person involved (e.g. a PIN), or by a physical property of a person (fingerprints or retina scans). Strong authentication requires at least two or more of these. A digital certificate provides strong authentication as it is a unique token (the

certificate itself) and requires a password (something known only to the owner) for its usage.

2. **Privacy:** In online commerce, privacy is the ability to ensure that information is accessed and changed only by authorized parties. Typically this is achieved via encryption. Sensitive data (such as credit card details, health records, sales figures etc.) are encrypted before being transmitted across the open internet – via email or the web. Data which has been protected with strong 128-bit encryption may be intercepted by hackers, but cannot be decrypted by them within a short time. Again, digital certificates are used here to encrypt email or establish a secure HTTPS connection with a web-server. For extra security, data can also be stored long-term in an encrypted format.
3. **Authorization:** Authorization allows a person or computer system to determine if someone has the authority to request or approve an action or information. In the physical world, authentication is usually achieved by forms requiring signatures, or locks where only authorized individuals hold the keys. Authorization is tied with authentication. If a system can securely verify that a request for information (such as a web page) or a service (such as a purchase requisition) has come from a known individual, the system can then check against its internal rules to see if that person has sufficient authority for the request to proceed. In the online world, authorization can be achieved by a manager sending a digitally signed email (an email stamped by their personal digital certificate). Such an email, once checked and verified by the recipient, is a legally binding request for a service. Similarly, if a web-server has a restricted access area, the server can request a digital certificate from the user's browser to identify the user and then determine if they should be given access to the information according to the server's permission rules.

4. **Integrity:** Integrity of information means ensuring that a communication received has not been altered or tampered with. Traditionally, this problem has been dealt with by having tight control over access to paper documents and requiring authorized officers to initial all changes made – a system with obvious drawbacks and limitations. If someone is receiving sensitive information online, he not only wants to ensure that it is coming from who he expects it to (authentication), but also that it hasn't been intercepted by a hacker while in transit and its contents altered. The speed and distances involved in online communications requires a very different approach to this problem from traditional methods. One solution is afforded by using digital certificates to digitally “sign” messages. A travelling employee can send production orders with integrity to the central office by using their digital certificate to sign their email. The signature includes a hash of the original message – a brief numerical representation of the message content. When the recipient opens the message, his email software will automatically create a new hash of the message and compare it against the one included in the digital signature. If even a single character has been altered in the message, the two hashes will differ and the software will alert the recipient that the email has been tampered with during transit.

5. **Non-repudiation:** Non-repudiation is the ability to guarantee that once someone has requested a service or approved an action, they cannot turn around and say “I didn't do that!”. Non-repudiation allows one to legally prove that a person has sent a specific email or made a purchase approval from a website. Traditionally non-repudiation has been achieved by having parties sign contracts and then have the contracts notarized by trusted third parties. Sending documents involved the use of registered mail, and postmarks and signatures to date-stamp and record the process of transmission and acceptance. In the realm of e-commerce, non repudiation is achieved by using digital signatures. Digital signatures which have been issued by a trusted authority (such as VeriSign) cannot be forged and their validity can be checked with any major email or web browser software. A digital signature is only installed in the personal computer of its owner, who is usually required to provide a password to make use of the digital signature to encrypt or digitally sign their communications. If a company receives a purchase order via email which has been digitally signed, it has the same legal assurances as on receipt of a physical signed contract.

4.5 Testing e-commerce security

The need for security testing of an organization arises due to two main factors. The primary factor is the importance of measuring the extent to which the security infrastructure implements the security policy and the security requirements of an organization. As the implementation of the security infrastructure needs human interventions, a proper security testing is needed to check out the existence of any “human error”. The other factor is the vulnerability of the existing security infrastructure to the new threats and exploits. In recent years, the rate of arrival of new types of threat and new exploits has been alarming with respect to the information security context. This leads to the need for periodical security testing by which the vulnerability of the existing

security infrastructure to the growing number of threats and exploits can be measured. The main objective of security testing, therefore, includes

1. Verification of the security requirement specification such as location of the asset(s), access control mechanism for the assets, operational context of the organization, existing system services and their access control mechanisms, and the connectivity within the organization and connectivity of the organization to the outside world
2. Verification of the configuration of the security tools specified in the security infrastructure i.e. whether the security tools are properly installed and configured to maintain the security of the asset
3. Verification of any gap between the proposed security infrastructure and the implemented security infrastructure
4. Verification of the limitation of the proposed security infrastructure with respect to the known vulnerabilities

Thus, there are two aspects of testing – compliance checking and penetration testing.

1. **Compliance checking:** In compliance checking, it is seen whether the security infrastructure, that has been implemented, matches the security policy of the organization. A semiautomated tool can be used to match the policies with the existing infrastructure.
2. **Penetration testing:** In penetration testing, it is seen whether the existing security infrastructure of the organization is sufficient to ward off all possible security threats. Various automated and semi-automated security tools like Retina, Nessus etc. are available for penetration testing. They try and penetrate the organization's network and generate a report on the vulnerabilities and threats that are present in the network. The feedback from the testing phase is used to upgrade the security infrastructure and security policy of the organization. After that, the testing is carried out again. Thus, security engineering is an iterative and dynamic process where all the phases need to be carried out at regular intervals to ensure the security of an organization.

Future Research

- Most e-commerce transactions currently are secured by the SSL (secure sockets layer) protocol, which is designed to encrypt data exchanges over the internet. While SSL is generally viewed as effective, an increasing number of vulnerabilities and other issues have spurred some e-commerce players to think about more secure standards. e-Commerce is evolving toward using XML (Extensible Markup Language) technology, which not only will serve as the foundation of many web services, but also will secure transactions between machines, relying on complex trust hierarchies to do so. SSL's foremost drawback is its reliance on certificate authentication at the user end, which requires users to have at least a basic understanding of the technology and processes involved in ensuring security. The same weakness is responsible for the demise of PKI (public key infrastructure) security; browser vulnerabilities and user ignorance often result in unsecured has not taken hold as widely as its predecessor. Instead, analysts predict that XML

Conclusion

- Electronic commerce is growing rapidly. A number of technologies have converged to facilitate the proliferation of e-commerce. The rapid advances in computer technology coupled with rapid acceleration in communication networks and the development of sophisticated software have revolutionized the way business is done. However, this is not sufficient to proliferate e-commerce applications. Proper management of enterprise information security resources is the need of the hour. We have, in this paper, put forth a "security engineering life cycle" approach to manage the information resources of an enterprise so that e-business can be carried out securely.

REFERENCES

1. COBIT 2000 Control objectives for information and related technology: COBIT, 3rd edn, July 2000, Released by the COBIT Steering Committee and the IT Governance Institute
2. Duggal P 2000 Cyberlaw in India –An analysis (New Delhi: Saakshartha)
3. ISO/IEC 2000 Information technology – Code of practice for information security management. ISO/IEC 17799: 2000(E)
4. Kalakota R, Whinston A B 1999 Frontiers of e-commerce (Reading, MA: Addison-Wesley/Longman)
5. Mazumdar C, BarikMS, Das S, Roy J, BarkatMA2003 Final technical report for project development of validated security processes and methodologies for web-based enterprises
6. Schneider G P, Perry J T 2001 Electronic commerce. Course Technology, Cambridge, MA
7. SSE-CMM2003 Systems security engineering capability maturity model. SSE-CMM, Model Description Document Version 3.0, June 15, 2003
8. Varshney U, Vetter R J, Kalakota R 2000 Mobile commerce: a new frontier. Computer Oct. : 32–38

WEBSITES

1. The house of secure e-commerce.
2. <http://www.istart.co.nz/index/HM20/PC0/PV21902/EX24014/AR25056>
3. e-Commerce security. www.upu.int/security/en/e-commerce-security-en.pdf
4. Legal aspects of e-commerce. <http://www.crimeresearch.org/library/Belousov-sep.html>
5. FAQ on Information Technology Act. <http://www.tamilnadunri.com/india/itpolicy/faq.html>
6. The state of e-commerce security. <http://www.newsfactor.com/perl/story/19462.html>